ABSTRACT OF THE DISCLOSURE

The trusted computer network is protected behind a gateway that includes a bastion host and screening router which blocks all URLs associated with the trusted network. The bastion host includes a remote client authentication mechanism and web proxy component that verifies and translates incoming URL requests from authenticated remote clients. Authentication is performed using one-time passwords that are stored on a portable storage device. The user configures the portable storage device by operating configuration software from the protected side of the gateway. The portable storage device also stores plug-in software to enable the client computer to properly retrieve the one-time password and exchange authentication messages with the bastion host. Further security is obtained by basing the one-time password on an encrypted version of the user's PIN. A symmetric key used to encrypt the PIN is stored in a protected area within the portable storage device.